University of Zurich[UZH]

**Zurich Open Repository and Archive**
University of Zurich
University Library
Strickhofstrasse 39
CH-8057 Zurich
www.zora.uzh.ch

Year: 2021

# Data ownership and data access rights: Meaningful tools for promoting the European digital single market

Thouvenin, Florent ; Tamò-Larrieux, Aurelia

DOI: https://doi.org/10.1017/9781108919234

Posted at the Zurich Open Repository and Archive, University of Zurich
ZORA URL: https://doi.org/10.5167/uzh-205448
Book Section
Published Version

Originally published at:
Thouvenin, Florent; Tamò-Larrieux, Aurelia (2021). Data ownership and data access rights: Meaningful tools for promoting the European digital single market. In: Burri, Mira. Big Data and Global Trade Law. Cambridge: Cambridge University Press, 316-339.
DOI: https://doi.org/10.1017/9781108919234

# 15

# Data Ownership and Data Access Rights

## *Meaningful Tools for Promoting the European Digital Single Market?*

*Florent Thouvenin and Aurelia Tamò-Larrieux**

### A INTRODUCTION

The digitalization and the increase in global trade significantly impact the economy and citizens of Europe. European policymakers are well aware of these developments and wish to unlock the potential of the digital economy through the EU's Digital Single Market Strategy.[1] One core goal of this strategy, promoted by the European Commission since 2015, is the pursuit of a free flow of data within the EU. Such a free flow should encourage the creation of and access to goods and services that – in their essence – collect and process vast amounts of data.

While the free flow of data is desirable from an economic perspective, as it maximizes the use of data by businesses throughout (and beyond) the EU, an entirely free flow of personal data goes against individuals' interests to exercise some control over the collection and use of their data by third parties. Therefore, a balance between economic and individual interests must be struck by creating a regime that ensures both. We call this desired balance an 'adequate free flow of data'. The term 'adequate' implies that a European digital economy should achieve more than economic welfare and simultaneously protect the interests of European citizens and consumers, especially their fundamental rights, such as the right to personal data protection. The balancing of interests could also benefit the digital economy, as it would promote the European citizens' trust and confidence in the

* Florent Thouvenin is Professor of Law, Chair for Information and Communication Law and Center for Information Technology, Society, and Law (ITSL), University of Zurich. Contact: florent.thouvenin@rwi.uzh.ch. Aurelia Tamò-Larrieux is Postdoctoral Fellow at the Institute for Work and Employment Research (FAA-HSG), University of St. Gallen. Contact: aurelia.tamo@unisg.ch. This contribution was completed at the end of December 2019. Literature and EU communications published after this date could only be considered selectively.

[1] European Commission, A Digital Single Market Strategy for Europe, COM(2015) 192 final, 6 May 2015; cf. also European Commission, A European strategy for data, COM(2020) 66 final, 19 February 2020.

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.

https://doi.org/10.1017/9781108919234.020

digital single market in order to enable the full exploitation of its potential. To achieve trust and confidence, legitimate boundaries to the free flow of data must be set.

Policymakers in the EU have debated whether the digital economy may benefit from the introduction of data ownership[2] and data access rights,[3] and legal scholars have analysed how such rights could lead to a digital economy benefitting all stakeholders. Yet policymakers and scholars have sometimes had different understandings of the term 'ownership', most often inadvertently. First, data ownership can be understood as a property right derived from civil law concepts of property in real estate and chattel, or intellectual property rights. This understanding of 'ownership' is how lawyers usually conceive the term. Second, data ownership can also be understood more broadly as a right that grants some control over data. It is this sort of ownership that non-lawyers typically have in mind when they advocate for the introduction of a 'data ownership right', most often (and again inadvertently) having only personal data in mind. With regard to personal data, this second understanding aligns with the approach taken in data protection law, namely in the EU's General Data Protection Regulation (GDPR),[4] which grants data subjects some control over their personal data. In contrast to data ownership, data access rights serve a different purpose – to empower individuals and businesses to obtain access to data that is of specific interest to them. Individuals have a legitimate interest in having access to personal data which is processed by businesses; the same is true for non-personal data that individuals have stored with a third party, such as a cloud provider. For businesses, access to data may be of key importance when offering innovative goods and services in the digital economy, as the use of specific data may be necessary to enter a new market or to remain competitive in an existing one.

In this chapter, we refrain from recapitulating the thorough academic debate on data ownership and data access rights.[5] Instead – and considering this book's broader perspective of big data and global trade – we look at the topic from a different angle and ask whether and how the concepts of data ownership and data access rights may

[2] See European Parliament, Resolution of 10 March 2016 on 'Towards a Thriving Data-Driven Economy' (2015/2612(RSP)), OJ C [2018] 50/50; European Commission, Towards a Common European Data Space, COM(2018) 232 final, 25 April 2018.

[3] See European Parliament, note 2; European Commission, note 2; OECD, *Data Driven Innovation – Big Data for Growth and Well-Being* (Paris: OECD Publishing, 2015), at 186–197.

[4] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), OJ L [2016] 119/1 [hereinafter: GDPR].

[5] For an overview, see R. H. Weber and F. Thouvenin, 'Dateneigentum und Datenzugangsrechte – Bausteine der Informationsgesellschaft?', *Zeitschrift für Schweizerisches Recht* 137 (2018), 43–74; J. Drexl et al., 'Data Ownership and Access to Data', Max Planck Institute for Innovation and Competition Research Paper No 10 (2016); F. Thouvenin, R. H. Weber, and A. Früh, 'Data Ownership: Taking Stock and Mapping the Issues', in M. Dehmer and F. Emmert-Streib (eds), *Frontiers in Data Science* (Boca Raton: CRC Press, 2018), at 111–145.

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

serve the goal of establishing an adequate free flow of data in the digital single market.

In the pursuit of the chapter's objective, we first map the policy goals contained within the EU's Digital Single Market Strategy. Upon this basis, we analyse how data ownership – understood as a property right – may serve the implementation of this strategy. Based on the insight that introducing property rights in data is unlikely to help implementing an adequate free flow of data, we examine in the following section of the chapter whether ownership as control over personal data is a viable alternative to the property rights approach. As a final step, we examine if, and under what circumstances, access rights to data already exist, or should be introduced, to allow individuals and businesses to use both personal and non-personal data. The last part concludes and explores paths towards strengthening data access rights, for instance, through the introduction of a compulsory licences regime.

## B THE DIGITAL SINGLE MARKET STRATEGY: BASIC FEATURES AND OBJECTIVES

In a nutshell, the goal of the EU Digital Market Strategy is to ensure that individuals and businesses have access to online services and products and that the requirements of fair competition, consumer and data protection as well as copyright are being fulfilled. In addition, no geo-blocking should occur within the Union.[6] In line with the general objective of fostering the internal market, the Digital Single Market Strategy aims to 'tear down the regulatory walls and move from 28 national markets to a single one',[7] while maintaining confidence in the digital economy. In order to promote the availability of good quality and interoperable datasets, EU policymakers seek to abolish inappropriate restrictions to the free flow of data across member states. Additionally, the European Commission wants to facilitate the value generation from datasets by training their citizens in the respective fields, by cooperating with industry and universities to determine the adequate skills required for the labour market and by promoting access to and transfer of knowledge amongst the private and the public sector.[8]

These statements show that the free flow of data is a key policy goal to enable the EU to compete in the global digital economy. But limitations are necessary to create a balanced approach that takes into account the needs of businesses and individuals

[6] See European Commission, note 1; European Commission, Shaping the Digital Single Market, available at https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market.

[7] European Commission, 'Tapping the Full Potential of the Data Economy for All Europeans', *The Commission's Contribution to the Leaders' Agenda*, May 2018, available at https://ec.europa.eu/info/sites/info/files/digital-single-market-all-europeans_en.pdf.

[8] European Commission, Towards a Thriving Data-Driven Economy, COM(2014) 442 final, 2 July 2014, at 5–6; see also European Commission, note 1, COM(2020).

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

alike. Some of the latter fear an ever-increasing collection and unrestricted processing of their personal data. In light of the power and information asymmetries between data processing entities and individuals, this fear is understandable and well-founded, as individuals are left with little or no control over how their personal data is being processed.[9] Thus, an important distinction needs to be made between the free flow of personal and non-personal data.

While some individuals fear a lack of control over their personal data, they hardly care about the collection and use of non-personal data. Accordingly, Europeans seem to be quite comfortable with the free flow of non-personal data.[10] In contrast, when it comes to personal data, an arguably central foundation of the digital single market is the establishment of a 'strong, consistent and comprehensive data protection framework for the EU'.[11] For users to have sufficient trust and confidence in the free flow of personal data, rules governing this flow must be adopted, and the European Commission sees the GDPR as the critical building block to do so. According to the commission, the GDPR is the central piece of legislation for the development of 'innovative and sustainable data goods and services',[12] and 'the foundation for the free flow of personal data in the EU', as it 'bans prohibitions and restrictions to the free movement of personal data for reasons connected with the protection of natural persons with regard to the processing of personal data'.[13] Even if restrictions to the free flow can be justified by other reasons (e.g. under taxation and accounting laws), the GDPR is seen as an important step to abolish data localisation restrictions – i.e., rules mandating local storage or processing activities. In fact, as data localization requirements of member states are a major obstacle to the free flow of data,[14] the abolishment of such restrictions is key to promote a flourishing European data economy.[15]

[9] See European Commission, Special Eurobarometer 431: Data Protection, dataset available at https://data.europa.eu/euodp/en/data/dataset/S2075_83_1_431_ENG.

[10] Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-personal Data in the European Union, OJ L [2018] 303/59, at paras. 59–68.

[11] European Commission, note 8, at 11.

[12] Ibid.

[13] European Commission, Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy, Accompanying the Document Communication Building a European Data Economy, COM(2017) 9 final, SWD(2017) 2 final, 10 January 2017, at 10.

[14] M. Burri and R. Schär, 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy', *Journal of Information Policy* 6 (2016), 479–511, at 500; M. Bauer, M. Ferracane, and E. van der Marel, 'Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization', CIGI Paper No 30 (2016); N. Cory, 'Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost', Information Technology and Innovation Foundation, 1 May 2017.

[15] European Commission, note 13, at 10; see also European Commission, Building a European Data Economy, COM(2017) 9 final, 10 January 2017, at 4–5.

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

Yet, while the GDPR certainly fosters a free flow of personal data within the EU by establishing a (relatively[16]) uniform regime in all EU member states, it also imposes substantial restrictions on the processing of personal data and thereby limits the free development and deployment of digital goods and services. While innovation remains possible, the GDPR has at least raised its costs, sometimes to a level making the deployment of innovative digital goods and services economically unfeasible.[17] These restrictions, however, are taken into account with the aim of protecting European citizens from the risks associated with the processing of their personal data. The tension between the free movement of personal data within the EU and the protection of the fundamental rights and freedoms of individuals is prominently highlighted in Article 1 GDPR, which addresses both goals in a separate paragraph. Interestingly, the European legislator is quite clear on the priority of the two objectives by stating that '[t]he free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data' (Article 1(3) GDPR). While it is doubtful whether this priority of objectives is actually put into action by the provisions of the GDPR, this statement supports our perspective that any (potential) regulation on personal and non-personal data should be analysed with regards to its ability to ensure an adequate free flow of data.

## C DATA OWNERSHIP

### I *Ownership as a Property Right*

#### 1 State of Research

The literature on data ownership as a property right is divided: While some authors argue that the current regulatory system is inadequate to protect individuals in the digital economy, others consider it adequate (or adequate enough) and therefore do not encourage the establishment of property rights in data. A first group of authors highlights the potential threats of big data and global trade for the protection of the

[16] Many flexibility clauses exist within the GDPR that allow member states to 'introduce national provisions to further specify the application of the rules' of the GDPR, introduce 'sector-specific laws in areas that need more specific provisions', or 'specify rules, including for the processing of special categories of data'. See Recital 10 GDPR.

[17] Chivot and Castro criticize the negative impact of the GDPR on innovation. See E. Chivot and D. Castro, 'The EU Needs to Reform the GDPR to Remain Competitive in the Algorithmic Economy', Center for Data Innovation, 13 May 2019; N. Wallace and D. Castro, 'The Impact of the New EU's Data Protection Regulation on AI', Center for Data Innovation, 27 March 2018; see also J. Drexl, 'Legal Challenges of the Changing Role of Personal and Non-personal Data in the Data Economy', Max Planck Institute for Innovation and Competition Research Paper No 23 (2018), at 11–12; for a different opinion, see R. Bastin and G. Wantz, 'The General Data Protection Regulation: Cross-Industry Innovation', *Deloitte Inside Magazine* 2 (2015).

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

fundamental rights and freedoms of European citizens. Data ownership, they argue, could help cushion some of the adverse effects of the digital economy.[18] The idea behind their string of reasoning is that, by assigning data to the person to whom it refers, the individual data 'owners' are put in a better negotiating position towards companies and thus a fairer distribution of the value created by the data processing can be ensured.[19] One strong proponent of a data ownership right even argues that such a right would empower individuals to combat the 'totalitarian digital appropriation strategies' of big tech companies.[20] Yet even proponents of data ownership as a property right acknowledge that the practical implementation of such a right remains unclear.[21] In fact, so far, only abstract calls for data ownership frameworks have been proposed.[22]

A second group of authors starts from the assumption that data is a public good.[23] This means that the use of data is non-rivalrous, as data can be used by an unlimited number of individuals simultaneously, and the use of one individual does not

[18] M. Amstutz, 'Dateneigentum: Funktion und Form', *Archiv für die Civilistische Praxis* 218 (2018), 439–551, at 489 et seqq.; see also F. Cheneval, 'Property Rights of Personal Data and the Financing of Pensions', *Critical Review of International Social and Political Philosophy* (2018), 1–23; I. Landreau et al., 'My Data Are Mine: Why We Should Have Ownership Rights on Our Data' (Paris: GenerationLibre, 2018), at 18 et seqq.; N. Purtova, 'The Illusion of Personal Data as No One's Property', *Law, Innovation, and Technology* 7 (2015), 83–111, at 86 et seqq.; E. Tjong Tjin Tai, 'Data Ownership and Consumer Protection', *Journal of European Consumer and Market Law* 7 (2018), 136–140, at 136 et seqq.

[19] M. Amstutz, 'Dateneigentum: Eckstein der kommenden Digitalordnung', *Neue Zürcher Zeitung*, 5 September 2018; see also H.-J. Naumer, 'Dateneigentum statt Datenkapitalismus', in Stiftung Datenschutz (ed), *Dateneigentum und Datenhandel* (Leipzig: Erich Schmidt Verlag, 2019), 233–239, at 234–236; H. Zech, 'Information as Property', *Journal of Intellectual Property, Information Technology and E-Commerce Law* 6 (2015), 192–197, at 197.

[20] Amstutz, note 19 (authors' own translation from German).

[21] Ibid.; also V. Janeček, 'Ownership of Personal Data in the Internet of Things', *Computer Law and Security Review* 34 (2018), 1039–1052, at 1052.

[22] See, e.g., proposal by the Federal Minister of Transport and Digital Infrastructure of Germany, Alexander Dobrindt, who called for a 'Data Law', which includes five basic principles: (i) defining data as a material commodity; (ii) which belongs to a particular person; (iii) providing transparent information about data processing; (iv) ensuring that public data is open data, and (v) enabling individuals to have payment options instead of sharing personal data. See Bundesministerium für Verkehr und Digitale Infrastruktur, Strategiepapier Digitale Souveränität: Wir brauchen ein Datenschutzgesetz in Deutschland!, available at www.bmvi.de/SharedDocs/DE/Artikel/DG/datengesetz.html. For an overview of different ownership framework proposals, see also J. Ritter and A. Mayer, 'Regulating Data as Property: A New Construct for Moving Forward', *Duke Law and Technology Review* 16 (2018), 220–277. For other proposals, see Landreau et al., note 18, at 76 et seqq.; also Cheneval, note 18, at 16; K.-H. Fezer, *Repräsentatives Dateneigentum – Ein zivilgesellschaftliches Bürgerrecht*, (Berlin: Konrad Adenauer Stiftung, 2018).

[23] T. Heymann, 'Rechte an Daten: Warum Daten keiner eigentumrechtlichen Logik folgen', *Computer Recht* (2016), 650–657, at 652–653; W. Kerber, 'A New (Intellectual) Property Right for Non-personal Data? An Economic Analysis', *GRUR Inernational* (2016), 989–998, at 992–993; F. Thouvenin, 'Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs', *Schweizerische Juristen-Zeitung* 113 (2017), 21–32, at 24; H. Zech, 'Daten als Wirtschaftsgut – Überlegungen zu einem "Recht des Datenerzeugers"',

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

interfere with the use of others. Against this background, introducing data ownership needs a convincing justification as such a property right would allow data owners to exclude others from using their data. According to these authors, property rights in public goods should only be granted in case of market failure, i.e. if data was not produced or used to a socially desirable degree.[24] However, in the age of big data one can hardly argue that a market failure with respect to the collection, creation, and processing of data exists. To the contrary, the exponential rise of the quantity and quality of data and its ubiquitous processing indicates that companies have enough incentives for collecting, processing, and trading data.[25] Even if incentives for the collection, processing, and trading of data exist, these activities might not lead to socially desirable outcomes. Nonetheless, it is doubtful whether these outcomes amount to an actual market failure and even more doubtful that such failure could be remedied by the introduction of propert rights in data.

A third group of authors excludes the introduction of data ownership rights from a fundamental rights perspective. They argue that the fundamental right to the protection of personal data safeguards the personality of data subjects, not their property.[26] Accordingly, a data subject cannot be 'regarded only or mainly as the owner of the data concerning him or her',[27] as such ownership would allow data subjects to trade their property rights away and thereby waive the guarantees of their fundamental rights.[28] From this perspective, granting property rights in personal data is impossible, as individuals are not free to waive or completely alienate the rights in their personal data. According to these authors, only some rights in their data could be transferred from data subjects to third parties, but not all of them.[29] For instance, a waiver of all data protection guarantees would not be permissible, but a numerus clausus of clearly defined 'leases' of personal data for specific purposes could be set in place.[30]

*Computer Recht* 31 (2015), 137–146, at 139; L. Determann, 'No One Owns Data', *Hastings Law Review* 70 (2018), 1–44, at 41.

[24] Drexl et al., note 5, at 2–3; W. Kerber, 'Governance of Data: Exclusive Property vs. Access', *International Review of Intellectual Property and Competition Law* 47 (2016), 759–762, at 760; Weber and Thouvenin, note 5, at 52–53.

[25] Drexl et al., note 5, at 2–3; J. Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access', Max Planck Institute for Innovation and Competition Reserach Paper No 13 (2016), at 30–31; F. Faust, 'Ausschliesslichkeitsrecht an Daten?', in Stiftung Datenschutz (ed), *Dateneigentum und Datenhandel* (Leipzig: Erich Schmidt Verlag, 2019), 85–100, at 99; Kerber, note 23, at 992–993; Weber and Thouvenin, note 5, at 52–53.

[26] S. Rodotà, 'Data Protection as a Fundamental Right', in S. Gutwirth et al. (eds), *Reinventing Data Protection?* (Berlin: Springer, 2009), 77–82, at 81; see also N. Purtova, 'Do Property Rights in Personal Data Make Sense after the Big Data Turn?', Tilburg Law School Legal Studies Research Paper No 21 (2017), at 8–9.

[27] Rodotà, note 26, at 81.

[28] Purtova, note 26, at 8; OECD, note 3, at 196.

[29] Purtova, note 26, at 8.

[30] Ibid.

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

With regard to the question whether the introduction of data ownership as a property right would foster an adequate free flow of data in the digital single market, other aspects are of crucial importance, namely the impact of such property rights on transaction costs and (as a result) on the use of data and the consequences for data subjects. We look in turn at these implications.

## 2 Analysis

A TRANSACTION COSTS The introduction of property rights in data would lead to a situation in which every transfer and use of data would have to be subject to a prior agreement with the owner of the data. First of all, the owner of the data to be used would have to be identified. Second, the potential user would have to negotiate with the owner and agree on whether and under what conditions the data can be used. Both the identification of the owner and the negotiation would lead to considerable transaction costs.[31]

Identifying the data owner might sometimes be straightforward but will more often be rather complicated. The former would be true for non-personal data which is controlled by a single entity, most often a business. The latter would apply to personal data. If one assumes that property rights in personal data would vest in data subjects, the use of large datasets containing data about a large number of individuals would quickly become very burdensome, as every data subject would have to be identified and contacted in order to negotiate the conditions for the use of their data. Although there are important differences between the transaction costs associated with the use of personal and non-personal data, the introduction of data ownership as a property right would increase transaction costs in all cases and thus hurt the free flow of data within the digital single market. With regard to personal data, one might argue that these transaction costs must be incurred to protect the interests of data subjects in having control over the use of their personal data, thus moving from a fully free flow to a somewhat restricted and more adequate free flow of personal data. Increasing transaction costs for using and trading non-personal data by introducing data ownership rights and thereby restricting the free flow of data cannot be justified.[32]

Some scholars have argued that property rights in data could (in theory) increase legal certainty and reduce transaction costs, as contract negotiations could start from a clear determination as to who owns what data.[33] However, an analysis of potential

[31] Weber and Thouvenin, note 5, at 53–54; Drexl, note 25, at 35.

[32] For an economic analysis of the introduction of a new property right on non-personal data, see Kerber, note 23, at 989; also Drexl et al., note 5, at 2 et seqq.

[33] See J. C. Sahl, 'Gesetz oder kein Gesetz, das ist hier die Frage – Zur Notwendigkeit gesetzlicher Regulierung in der Datenökonomie', *Privacy in Germany* 4 (2016), 146–151, at 149; Kerber, note 23, at 994–995.

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

criteria for allocating property rights in data shows that it is far from obvious which criteria should be applied to determine ownership, especially with regard to non-personal data.[34] While it seems intuitive that data subjects should be the owner of personal data relating to them, it is less clear if businesses collecting such data should likewise have some ownership over the data accumulated in their systems. Besides, personal data quite often relates to more than one individual; for instance, a picture of a group of people or the genetic data of one person which always of data about that person's parents, grandparents, siblings, infants, etc. Concerning the difficulties of identifying and applying a suitable criterion for allocating property rights in data, introducing data ownership rights would rather raise than reduce transaction costs and limit the free flow of data in the digital single market.

b consequences for data subjects The introduction of property rights in personal data would most probably have negative consequences for data subjects. Even if data controllers most often process personal data based on legitimate interests (Article 6(1)(b), (c) and (f) GDPR),[35] another important foundation for the lawfulness of processing is the data subjects' consent (Article 6(1)(a) GDPR). If the processing is based on consent, data subjects can – at least in theory – decide whether businesses may use their personal data by accepting their terms and conditions and/or their privacy policies. In doing so, they 'trade' their personal data in exchange for 'free' goods and services. However, under the current data protection regime, consent can be withdrawn by data subjects at any time (Article 7(3) GDPR), thereby enabling them to prohibit the future processing of their personal data, if they reconsider their previous decision.

Granting property rights in personal data would mean that these property rights could be transferred to third parties.[36] Given this possibility, we have to expect that businesses would request that users of their services transfer those property rights to them – just as they currently request users to allow for an all-encompassing use of their data through consent. As opposed to the situation today, however, businesses that acquire their users' property rights in their personal data would be able to exclude these users from using their personal data themselves and from exercising the limited amount of control they have today. As a result, introducing property rights in personal data would substantially weaken the position of data subjects – which is the contrary of what people advocating for such rights want to achieve. While the option to transfer ownership rights in personal data might have a positive impact on the free flow of such data, the interests of data subjects in being able to exercise some control over the processing of their personal data would be neglected.

[34] Thouvenin et al., note 5, at 116–117; Drexl, note 25, at 38 et seqq.

[35] F. Thouvenin, 'Datenschutz auf der Intensivstation: Befund, Diagnose und Therapie', *digma* (2019), 206–213.

[36] Thouvenin, note 23, at 26.

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.020

As a consequence, the introduction of property rights in personal data would compromise the goal of establishing an adequate free flow of data.

### 3 Interim Conclusion

The analysis shows that introducing data ownership as a property right does not promote the goals of the Digital Single Market Strategy. For non-personal data, granting property rights would raise transaction costs and thereby deter or at least encumber its free flow. Accordingly, legislators should not introduce any property right in such data. Moreover, there are no reasons why the free flow of non-personal data should be restricted by any other legal means. On the contrary, the full potential of non-personal data can be achieved if that data is shared amongst businesses, for instance, through the granting of access rights, as discussed later.

While property rights in personal data would also increase transaction costs, these costs could be justified with regard to the goal of protecting the interests of data subjects in having some control over the use of their personal data. However, the granting of property rights in personal data would lead to a different and quite severe problem: Since property rights in personal data could be transferred to any third party, businesses would most likely make sure that their users transfer these property rights when using their services. Consequently, data subjects would not only lose control over their personal data but businesses, as the owners of said data, could even forbid them to further use their personal data altogether. Such a scenario would undermine the policy goal of establishing an adequate free flow of personal data within the EU.

## II *Ownership as Control*

### 1 Preliminary Remarks

The concept of 'ownership as control' is generally accepted and well-established for personal data and is usually called 'informational self-determination' or 'informational autonomy'.[37] These notions refer to the individual's right to determine which information about them is disclosed to others and for what purposes such information will be used.[38] Data protection laws are generally based on these concepts.

[37] See Recital 7 GDPR; also Purtova, note 26, at 6 et seqq.; H. U. Vrabec, 'Uncontrollable: Data Subject Rights and the Data-driven Economy', PhD thesis, University of Leiden (2019), at 105 et seqq. Note that the principle of 'informational self-determination' has been criticized in the literature. See H. P. Bull, *Informationelle Selbstbestimmung – Vision oder Illusion?* (Tübigen: Mohr Siebeck, 2011); Thouvenin, note 35; W. Veil, 'The GDPR: The Emperor's New Clothes – On the Structural Shortcomings of Both the Old and the New Data Protection Law', *Neue Zeitschrift für Verwaltungsrecht* 10 (2018), 686–696.

[38] German Constitutional Court (census decision) in 1983 (BVerfGE 65,1).

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

The GDPR is even quite explicit about this underlying rationale by stating that 'natural persons should have control of their own personal data' (Recital 7). The concept of control is most clearly expressed in the condition of consent for the lawfulness of data processing (Article 6(1)(a) GDPR) and in the individual rights of the data subjects (Articles 12 et seqq. GDPR). In the following sections, these concepts are analysed further to assess whether ownership as control is a meaningful approach to establish an adequate free flow of personal data.

## 2 Implementation

A CONSENT At the stage of collection, consent and the right to information are the fundamental principles within the GDPR for granting control. In order to be compliant with the GDPR, consent must represent a 'freely given, specific, informed and unambiguous indication' by the data subjects by which they state or clearly affirm their agreement with the processing of personal data relating to them (Article 4(11) GDPR). It is key that the data subjects have a real choice to agree or disagree to the data collection. Such a choice is challenged in cases of power imbalances or if consent is the condition for the performance of a contract or for the provision of a service (Article 7(4) GDPR).[39] Similarly, any form of deception, intimidation, or significant negative consequences for the data subjects if they do not consent or later withdraw consent will fail to fulfil the requirement of a freely given consent.[40]

Consent is given on an informed basis if the data subjects are able to understand who processes what data for which purpose(s), if they are made aware of their right to withdraw consent, and if they obtain information about the use of their data for automated decision-making, as well as on the risk associated with a transfer of the data to an unsafe third country.[41] More often than not, the necessary information is provided in the controllers' privacy policy or as a specific part of the general terms of service. In either case, the information must be provided in an intelligible and accessible form, using clear and plain language (Article 7(2) GDPR).

Due to the complexity of digital goods and services, being adequately informed about the data processing is very challenging and it can be argued that due to an overload of consent notices, data subjects no longer make active, informed choices

[39] See Article 29 of Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, 28 November 2017 [hereinafter, Working Party 29 Consent Guidelines], at 5–6; E. M. Frenzel, 'Art. 7 DSGVO: Bedingungen für die Einwilligung', in B. P. Paal and D. Pauly (eds), *Datenschutz-Grundverordnung*, 2nd edn (Munich: C. H. Beck, 2018), 107–115.

[40] Ibid.

[41] Working Party 29 Consent Guidelines, note 39, at 13.

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

but merely agree to such notices when they are asked to do so.[42] Because users often 'blindly' agree to notices that pop up on their screens, the ability to withdraw consent (Article 7(3) GDPR) at any given time becomes (at least in theory[43]) an important redress mechanism for such situations and extends the control of data subjects beyond the stage of data collection to the entire data lifecycle.

B DATA SUBJECTS' RIGHTS Next to consent, data subjects' rights provide individuals with control over the use of their data, which is why they are also referred to as 'control rights'.[44] These rights apply notwithstanding whether the processing is based on consent or if another legal basis applies (see Article 6(1)(b-f) GDPR).

Data subjects' rights include

- the right to information (Articles 13 and 14 GDPR), which lists the (comprehensive) information that data controllers must provide to data subjects when collecting their data;
- the right access (Article 15 GDPR), which grants data subjects the right to get a copy of the personal data (in a commonly used electronic format) from the data controller and the right to obtain similar information on the processing of their data as provided for under the right to information;
- the right to rectification (Article 16 GDPR), which empowers data subjects to rectify inaccurate or complete incomplete personal data;
- the right to erasure (Article 17 GDPR), which allows data subjects to have their data erased by the data controller in specific circumstances, namely if the data subject withdrew consent or if the data is no longer necessary for the purposes it was collected for;
- the right to restriction of processing (Article 18 GDPR) in specific circumstances, namely if the accuracy of the data is contested or if the data subject has objected to the processing;
- the right to data portability (Article 20 GDPR), which enables data subjects to receive their data in a machine-readable format or to transmit it to any third party;
- the right to object (Article 21 GDPR) to data processing which is based on public or legitimate (private) interests on grounds relating to their particular situation;

[42] B. Schermer, B. Custers, and S. van der Hof, 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection', *Ethics and Information Technology* 16 (2014), 171–182, at 171–172.

[43] See B. Custers, 'Click Here to Consent Forever: Expiry Dates for Informed Consent', *Big Data and Society* 3 (2016), 1–6. Custers describes the practical challenges that the withdrawal of consent faces in the data economy. He notes that users typically do not withdraw consent to free accounts but merely stop using the service.

[44] Vrabec, note 37, at 111.

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.020

- and the right not to be subject to automated decision-making (including profiling) when such an automated decision produces legal effects or similarly significantly affects a data subject (Article 22 GDPR).

Boundaries to these data subjects' rights are set within the GDPR, either within the data subjects' rights themselves or through Article 11 GDPR. The latter limits the rights of the data subject when the data controller is unable to reidentify a data subject within its datasets. While the rights to access, rectification, erasure, restriction, and portability do not apply in such cases, the data subjects' right to information, to objection, and to not being subject of automated decision-making still prevail (Article 11(2) GDPR).

## 3 Analysis

When personal data is being processed, the GDPR provides a some control to data subjects: Consent is one of the two most important lawful bases of processing, thereby handing the decision whether personal data is processed to the data subject. In addition, data subjects have a well-developed set of rights that allow them to be informed about, to exert some control and quite often also to inhibit the processing of their data by the data controller.

However, the GDPR only provides an amount of control. Most importantly, the lawfulness of the processing can be (and often is) based on the legitimate interests of the controller or public interests; in these instances, the processing of personal data is warranted without the consent and even against the will of the data subject.[45] Besides, control is also limited, as many of the data subjects' rights come with essential restrictions. For instance, the right to erasure is only granted if one out of a limited set of situations is given, namely if personal data is no longer necessary in relation to the purpose for which it was collected (Article 17(1)(a) GDPR), if the data subject withdraws consent and there is no other legal grounds for the processing (Article 17(1)(b) GDPR), or if the data has been unlawfully processed (Article 17(1)(d) GDPR). Another example is the right to data portability, which is limited if the personal data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 20(3) GDPR).

By providing a limited amount of control to data subjects, the GDPR aims to strike a balance between facilitating the free flow of personal data and ensuring that

[45] F. Ferretti, 'Data Protection and the Legitimate Interests of Data Controllers: Much Ado about Nothing or Winter of Right?', *Common Market Law Review* 51 (2014), 843–868, at 856. In cases where processing is based on legitimate interests pursuant to Article 6(1)(b-f) GDPR and the conditions for the right to erasure (Article 17 GDPR) to restriction (Article 18 GDPR) or to object (Article 21 GDPR) toare not met, personal data may be processed even if data subject opposes such processing.

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.020

data subjects can exercise control with respect to the processing of their data (Recital 7 GDPR). Thereby, the law balances conflicting interests of data subjects and data controllers and aligns them with the ideal of an adequate free flow of personal data. The ideal of a 'free flow' is achieved by establishing a (mostly) harmonized data protection law framework within the EU, while the adequacy of the free flow is guaranteed by enshrining the notion of ownership as (adequately limited) control over personal data.

Compared with the property rights model, ownership as control takes a more balanced approach. In particular, data access rights are seen as a way forward to enable a more (adequate) free flow of personal data within the EU.[46]

## D DATA ACCESS RIGHTS

### I *Access by Individuals*

#### 1 Access to Personal Data

Data subjects have a legitimate interest in having access to personal data others process about them. Therefore, the GDPR provides data subjects with a right to receive information about the purposes of the processing, the categories of personal data being processed, as well as – if determinable – the period for which the data will be stored (Article 15(1) GDPR). Amongst others, such access empowers individuals to verify the lawfulness of the processing of their personal data (Recital 63 GDPR). More important – from the perspective of the free flow of data – is the right of data subjects to receive a copy of their data from the data controller; if such request is made by electronic means, the controller shall provide the data in a commonly used electronic form (Article 15(3) GDPR). Where possible, the controller should even grant data subjects remote access to a secure system, which provides them with direct access to their personal data (Recital 63 GDPR). The right to obtain a copy is only restricted if such right adversely affects the rights and freedoms of others (Article 15(4) GDPR), namely if providing a copy of the data would harm trade secrets or intellectual property rights (Recital 63 GDPR). At least theoretically, data subjects are thus able to collect and later use all the data that others have about them.

The explicit and fully fledged right to obtain a copy of the personal data is closely linked to the right to data portability,[47] which the GDPR grants on top of the right of access if the processing is carried out by automated means (Article 20 GDPR). The latter allows data subjects to (re)claim the personal data they provided to the

[46] See also H. Richter and R. M. Hilty, 'Die Hydra des Dateneigentums – eine methodische Betrachtung', in Stiftung Datenschutz (ed), *Dateneigentum und Datenhandel* (Leipzig: Erich Schmidt Verlag, 2019), 241–259, at 256; European Commission, note 2; OECD, note 3.

[47] Vrabec, note 37, at 216.

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

controller in a structured, commonly used and machine-readable format (Article 20 (1) GDPR). Data subjects may themselves receive their personal data, transfer it, or have it, directly transmitted to another controller, if technically feasible. However, the scope of the right to data portability is restricted to data 'provided' by the data subject and to the instances of processing based on consent or a contract.[48] As a consequence, all data inferred from the personal data or information predicted by data controllers, will not be subject to this right.[49] However, the right of access, which is not restricted to data provided by the data subject, may empower data subjects with a right to get a copy of this data all the same.

## 2 Access to Non-personal Data

Individuals might also have legitimate interests in having access to non-personal data (e.g. text documents, spreadsheets, presentations, or other files that do not contain personal information) that they stored with a service provider, such as a cloud storage or a webmail provider. Such data will most often be processed on a contractual basis. These contracts grant users access to the service providers' servers to upload and access their files. The applicable terms of service of cloud service providers usually state that the users own the files and that they have a right to access their files, while cloud providers most often reserve the right to access, store, and scan these files (see for instance the terms of service of Dropbox or Google Drive). If the terms of service do not explicitly provide for a user's right of access, courts might derive such right from the underlying contract given that granting access to one's data is the very nature of such contracts. Accordingly, users should have a right to access non-personal data they provided to a service provider in most cases.

If non-personal data has been stolen, e.g., by hacking a user's device, criminal sanctions apply. In addition to these sanctions, tort law may give users a right to reclaim their non-personal data from the ones that stole it from them.[50] Even if such claims may be difficult to enforce in practice, the legal basis for access is given.

[48] The term 'provided' can be interpreted restrictively, meaning that it concerns only personal data that the data subject explicitly provided in an explicit form, or extensively, including data that the controller collects upon consent or according to a contract (e.g. GPS, cookies, preferences). See P. De Hert et al., 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services', *Computer Law and Security Review* 34 (2018), 193–203, at 199; P. De Hert, 'The Future of Privacy: Addressing Singularities to Identify Bright-Line Rules That Speak to Us', *European Data Protection Law Review* 4 (2016), 461–466. De Hert argues that when dealing with fundamental rights, we should favor the interpretation that is most beneficial for individuals. Likewise, the Working Party 29 in its Guidelines on the Right to Data Portability argues for a broad interpretation of the term 'provided'. See Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability, 13 December 2016 [hereinafter, Working Party 29 Data Portability Guidelines].

[49] De Hert et al., note 48, at 199.

[50] For a legal analysis under Swiss law, see Weber and Thouvenin, note 5, at 58–59; with reference to M. Eckert, 'Digitale Daten als Wirtschaftsgut: digitale Daten als Sache',

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

## 3 Analysis

Although the law does not provide for a general right of access to all sorts of data, individuals seem to be able to get access to 'their' data in most instances where access can reasonably be required. At the same time, data controllers and processors may only process their personal data in accordance with the requirements of the GDPR. Accordingly, from the perspective of the individuals, an adequate free flow of their data seems to be granted (at least in theory).

This is especially true when personal data is being processed as data subjects can draw upon the various control rights established in the GDPR, as discussed earlier. Next to the right of access, the right to data portability is seen as a powerful means to strengthen individual control.[51] In theory, this right should ensure that data subjects 'play an active role in the data ecosystem'[52] and enable them to break up service lock-ins in the digital economy (especially in social media). In this sense, data portability is seen as a means to foster competition,[53] while simultaneously ensuring an adequate free flow of personal data. However, it is more than doubtful that these goals can be achieved, since the vast majority of data subjects have so far only reluctantly made use of their individual rights.[54] Also, the mere right to data portability will hardly suffice to overcome the strong network effects which exist in some sectors, especially in social media platforms.[55] Nevertheless, the right of access and the right to data portability may prove useful for switching providers in other sectors, such as email or cloud storage providers.

*Schweizerische Juristen-Zeitung* 112 (2016), 245–249 and U. Hess-Odoni, 'Die Herrschaftsrechte an Daten', *Jusletter*, 17 May 2004. Weber and Thouvenin (note 5, at 59) provide also references to German literature elaborating on the right to reclaim stolen data; amongst others, see T. Hoeren, 'Dateneigentum – Versuch einer Anwendung von § 303a StGB im Zivilrecht', *Multimedia und Recht* 8 (2013), 486–491.

[51] Recital 68 GDPR.

[52] Working Party 29 Data Portability Guidelines, note 48, at 4, footnote 1.

[53] Ibid., at 3–4; De Hert et al., note 48, at 195.

[54] See J. Ausloos and P. Dewitte, 'Shattering One-Way Mirrors: Data Subjects Access Rights in Practice', *International Data Privacy Law* 8 (2018), 4–28, at 5; Vrabec, note 37, at 257 et seqq. Note that there is not much data available on the number of requests (e.g. access, restriction, portability) made by data subjects to individual data controllers. Search engine providers only publish the number of erasure requests received, e.g., Google publishes erasure requests made in every country. See Google, 'Requests to Delist Content under European Privacy Law', Google Transparency Report, available at https://transparencyreport.google.com/eu-privacy/overview?hl=en. Data protection authorities in the EU have noticed an increase of complaints brought forward by individuals, see, e.g., Commission nationale de l'informatique et des libertés (French Data Protection Authority), Presentation of the 2018 Activity Report and 2019 Issues of the French Data Protection Authority, 15 April 2019, available at www.cnil.fr/en/presentation-2018-activity-report-and-2019-issues-french-data-protection-authority. Note that websites such as www.datarequests.org/ have been created to facilitate obtaining access to personal data from companies. It remains unclear whether such sites have led to an increase of data subjects' requests.

[55] European policymakers have recently proposed legislative initiatives to tackle some of these issues, e.g., by means of the Digital Services Act (DSA) and Digital Markets Act (DMA). See

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

When non-personal data that belongs to a particular individual is being processed, data can most often be accessed based on contractual norms and sometimes based on tort law. While these access rights are much less comprehensive than the access rights for personal data, the latter may promote access to non-personal data for two reasons. First, because service providers have to build their systems in a way that allows them to extract the personal data of their users to comply with the right of access granted in data protection law, they need to build their systems in a way that enables them to identify and distinguish personal from non-personal data. Within this process non-personal data that belongs to an individual, such as text documents, can be identified and extracted as well. Second, it is often hard (or even impossible) to distinguish personal and non-personal data, and both types of data are often present in a single file, e.g. in a document that contains information about its author or in an email that always contains information about recipient and sender (at least in the metadata). Accordingly, it might be easier for service providers to provide all the data that belongs to an individual (whether personal or non-personal) if the said individual requests access to their personal data. It, therefore, seems that the current legal situation should also ensure an adequate free flow of non-personal data that belongs to an individual.

## II *Access by Businesses*

### 1 Preliminary Remarks

Until today there are no general data access rights for businesses, neither with regard to data held by other businesses nor for data held by government agencies. But, of course, businesses can grant each other access to data on the basis of a contract. The default for businesses, however, seems to be that data is regarded as an asset that should not be shared with others. The general approach of collecting and analysing data in-house and via sub-contractors, and ensuring that this data stays within organizations and is not traded with other businesses,[56] is an essential impediment to the free flow of data and harms the overall digital economy.

As a public good, data could be used by an unlimited number of businesses simultaneously and the use by one business would not interfere with the use of others. Accordingly, granting access rights to businesses would be a meaningful way to enable broader use of data, unravel its potential, and foster competition. While this applies to all sorts of businesses, it is especially true for start-ups and small- and medium-sized enterprises (SMEs), which could benefit from the access to data for developing innovative digital

European Commission, Proposal for a Single Market for Digital Services (Digital Services Act) Amending Directive 2003/31/EC, COM(2020) 825 final, 15 December 2020; European Commission, Proposal on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), COM(2020) 842 final, 15 December 2020.

[56] European Commission, note 13, at 15.

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

goods and services.[57] It is therefore not surprising that both the European Commission[58] and the OECD[59] are promoting the digital economy via access rights.

Even if no harmonized legal framework granting access rights for businesses exists, some sector-specific regulations can remedy specific problems. Besides, competition law contains generally applicable rules that may allow businesses to request access to data in some situations. More recently, the introduction of compulsory licences has been promoted in the literature as a new and promising way to establish access rights for businesses.

## 2 Implementation

A SECTOR-SPECIFIC REGULATIONS There are three types of sector-specific regulations granting access rights to data: (i) regulations granting government agencies access to data held by businesses; (ii) regulations that provide businesses access to data held by government agencies; and (iii) regulations providing businesses access to data held by other businesses. The first type of access rights ensures that government agencies have access to the data they need to perform their tasks and to take well-informed decisions.[60] Such access rights are common in many EU member states[61] but they are not the subject of this chapter, the enquiry of which is limited to access rights of businesses. The second type of access rights is a means to make better use of the data collected by government agencies by enhancing the reuse of such data. The third type mainly aims at fostering competition.

The most prominent example of the second type of access rights is the EU's Public Sector Information Directive.[62] According to this directive, this data must be

[57] Drexl et al., note 5, at 8.

[58] European Commission, note 2; see also Richter and Hilty, note 46, at 256.

[59] OECD, note 3.

[60] A. Früh, 'Datenzugangsrechte: Rechtsrahmen für einen neuen Interessensausgleich in der Datenwirtschaft', *sic!* 10 (2018), 521–539, at 528 et seqq. with reference to European Statistical System, 'Access to Privately Held Data', Position Paper, November 2017.

[61] In France, for instance, the government has a right to access privately held data that are relevant for establishing public statistics (Article 19 Loi 2016-1321 du 7 octobre 2016 pour une Répulique numérique, NOR: ECFI1524250L, JORF 0235 du 8 octobre 2016, texte 1). Overall, France has been pushing for access rights to privately held data in various sectors, such as for scanner data of retailers, in order to improve the quality of the standard Consumer Price Index, for mobile phone data to measure the mobility of people within local areas, or for data on tourist accommodations offered by individuals on the Internet. Other EU member states – such as Italy, the Netherlands, and Poland – are likewise establishing regulations allowing statistical authorities to access scanner data of large retailers and supermarkets. In Estonia, government agencies have access to data from smart electricity meters in order to produce electricity consumption statistics of households and businesses and accordingly plan for future electricity needs. See European Statistical System, note 59, at 8 et seqq.

[62] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83.

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

freely available for reuse and public sector bodies are not allowed to charge more than marginal cost for such reuse.[63] However, one could argue that if private businesses profit from data provided by the government, the general public should in return obtain some benefits from the data that businesses generate through the use of government data, or that at least government agencies obtain access to such data at marginal costs.[64]

The third type of access rights is not very widespread, at least until today. A case in point is the maintenance work on cars which often depends on access to data about the car. This case is governed by Regulation 715/2007 of the EU.[65] In order to foster competition in the market for car maintenance, manufacturers of cars must provide unrestricted and standardized access to specified information to repair workshops through websites using a standardized format in a readily accessible and prompt manner (Article 6 Regulation 715/2007). For doing so, the manufacturers can charge a 'reasonable and proportionate fee' (Article 7 Regulation 715/2007). Another example is the EU Directive 2015/2366 on payment services in the internal market,[66] which enables payment service providers to get access to data held by banks in order to facilitate their market access.[67]

B COMPETITION LAW In addition to sector-specific regulations, competition law contains generally applicable rules that may arguably serve as access right. In practice, however, competition law is not a workable solution, for several reasons:[68]

[63] European Commission, 'Digital Single Market: EU Negotiators Agree on New Rules for Sharing of Public Sector Data', *Press Release*, 22 January 2019.

[64] Früh, note 59, at 525–526. In order to prevent public sector information being locked in by private companies that work for the government, the EU will establish safeguards that will reinforce transparency and limit the conclusion of agreements which could lead to exclusive reuse of public sector data by private partners. See European Commission, note 62.

[65] Regulation No 715/2007 of the European Parliament and of the Council of 20 June 2007 on Type Approval of Motor Vehicles with Respect to Emissions from Light Passenger and Commercial Vehicles (Euro 5 and Euro 6) and on Access to Vehicle Repair and Maintenance Information, OJ L [2007] 171/1; C. König, 'Der Zugang zu Daten als Schlüsselgegenständen der digitalen Wirtschaft', in M. Hennenmann and A. Sattler (eds), *Immaterialgüter und Digitalisierung: Junge Wissenschaft zum Gewerblichen Rechtsschutz, Urheber- und Medienrecht* (Baden-Baden: Nomos, 2017), 89–104, at 94.

[66] Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC, OJ L [2015] 337/35 [hereinafter: Directive 2015/2366].

[67] Article 35 Directive 2015/2366.

[68] For an overview of the failures of competition law to grant access to privately held data, see J. Drexl, *Data Access and Control in the Era of Connected Devices*, Study for the European Consumer Organisation (Brussels: BEUC, 2018), at 4 and 36 et seqq.; Drexl et al., note 5, at 9–10; Früh, note 59, at 532 et seqq.; A. Früh, 'Zum Bedarf nach Datenzugangsrechten', *Jusletter IT Flash*, 11 December 2017; B. Lundqvist, 'Big Data, Open Data, Privacy Regulation, Intellectual Property and Competition Law in an Internet of Things-World: The Issue of Access', in M. Bakhoum et al. (eds), *Personal Data in Competition, Consumer*

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

First, with regard to access rights, competition law only comes into play in respect of businesses with a dominant position; even if this condition is met, access can only be requested in case of an abuse of such dominance (Article 102 TFEU). Second, the traditional criteria for defining the relevant market are not very helpful for defining markets in the data economy.[69] Third, and most importantly, competition law cases take a very long time to be decided, sometimes up to ten years.[70] It is obvious that businesses requesting access to data need much faster procedures to enforce their rights. Therefore, competition law is not a meaningful way for granting access to data.

c COMPULSORY LICENCES A promising way forward for ensuring access to data is the granting of compulsory licences as known in intellectual property law. As opposed to competition law, where courts define the conditions of granting a licence ex post, the conditions of such compulsory licences are defined ex ante. The difficulty here rests in establishing a system that considers the interests of all businesses involved, the one requesting and the one granting access, especially the latter's interest in securing its trade secrets.[71]

A general right of access to data would have to be regulated in a generally applicable body of law. A suitable and convincing approach is introducing such a right in trade secrets law. This previously quite heterogeneous body of law has recently been harmonised by the EU's Trade Secrets Directive.[72] The directive contains an expansive notion of trade secrets embracing all secret information (i.e. information not generally known or readily accessible) that has commercial value because it is secret and is subject to reasonable steps to keep it secret.[73] This definition encompasses most data held by businesses. Accordingly, amending trade secrets law would be a promising way to introduce general compulsory licences for granting access to data. While such an approach would be rather broad, compulsory licences could also be granted in sector-specific regulations, such as in telecommunications or energy acts, or in a potential regulation of platforms, covering search

*Protection and Intellectual Property Law: Towards a Holistic Approach?* (Berlin: Springer, 2018), 191–214, at 202–203.

[69] Drexl, note 67, at 36; Lundqvist, note 67, at 202–203.

[70] Früh, note 59, at 535; for an illustrative example, see R. Podszun, 'Lizenzverweigerung – Ernstfall im Verhältnis von Kartell und Immaterialgüterrecht', in P. Matousek, E. Müller, and T. Thanner (eds), *Jahrbuch Kartell- und Wettbewerbsrecht* (Wien: Neuer Wissenschaftlicher Verlag, 2010), 57–76.

[71] Früh, note 59, at 528, 530; A. Wiebe, 'Von Datenrechten zu Datenzugang – Ein rechtlicher Rahmen für die europäische Datenwirtschaft', *Computer und Recht* 33 (2017), 87–93, at 92.

[72] Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) against Their Unlawful Acquisition, Use and Disclosure, OJ L [2016] 157/1 [hereinafter, Directive 2016/943].

[73] Article 2(1) Directive 2016/943.

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.020

engines or social media providers. In any case, access rights should not be granted for free. Rather, any business making use of its right of access should pay a fair, reasonable, and non-discriminatory (FRAND) compensation to the business that has collected, stored, and curated the data.[74]

Even if compulsory licences are considered a meaningful way of granting access to data, many things are still unclear. For example, one would have to define the conditions for granting such a licence and its scope (i.e., the data which is covered), as well as the purpose for which the data may be used if access is granted.[75] Today's case law contains some hints to address these important questions – the need for having access to data for entering a secondary market.[76] Other conditions could relate to single source data situations or some degree of market power of the business that should grant access. Also, one would have to decide whether a compulsory licence includes the right to get a copy of the data or whether such right should be limited to using and analysing the data on the machines of the trade secret owner. Lastly, and most importantly, even if compulsory licences are considered a suitable mechanism for granting access rights, it remains unclear if granting such licences is justified.

The most important argument in favour of introducing compulsory licences is undoubtedly the fact that data is a public good, as discussed earlier. Also, the business of most companies is not selling data to their customers but providing services that are based on data. As a consequence, granting access to data does not necessarily have a negative impact on the market share of the business that has to provide access. If this should be the case, one could consider restricting access to businesses that are not direct competitors but active in a secondary or even in an entirely different market.

The most important argument against granting access rights is the risk of undermining incentives for collecting, storing, and curating data. However, for the time being, it is hard to imagine that well-defined access rights would actually undermine such incentives to a relevant degree.

## 3 Analysis

Access rights for businesses are a meaningful way to enhance the free flow of data in the digital single market in order to foster innovation and strengthen the competing power of European companies. While competition law is not a workable solution,

[74] European Commission, note 13, at 39; Früh, note 59, at 537; Früh, note 67.

[75] Früh, note 67.

[76] Lundqvist, note 67, at 202–203 with reference to Joined Cases C-241/91 and C-242/91, *Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP)* v. *Commission of the European Communities* [1995], ECLI:EU:C:1995:98; C-418/01, *IMS Health GmbH & Co. OHG* v. *NDC Health GmbH & Co. KG* [2004], ECLI:EU:C:2004:257; T-201/04, *Microsoft Corp.* v. *Commission of the European Communities* [2007], ECLI:EU:T:2007:289.

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

two complementary approaches seem quite promising: First, trade secrets law could be amended to include compulsory licences, which allow businesses to claim access to data held by other businesses. Given the very broad scope of application of trade secrets law, this approach would allow to establish a general right of access to data. In order to protect the interests of businesses that have to grant access, relatively strict conditions would have to be designed and businesses requesting access would have to pay an appropriate licence fee. Second, sector-specific regulations could grant specific access rights. In such regulations, the conditions for claiming access could be modified and be either stricter or more lenient than in trade secrets law and certainly more specific, also with regard to the calculation of the licence fee. In addition, there might be situations in which access should be granted for free or only if the businesses involved grant each other access on a mutual basis (cross-licence). The combination of these two approaches would allow for a comprehensive regime of access rights, ensure an appropriate balancing of interests, and help establish an adequate free flow of data amongst businesses in the digital single market.

For the free flow to be fully adequate the interests of the individuals represented in the data must be taken into account as well. This is ensured by the application of the GDPR, which regulates virtually all processing of personal data by businesses (Article 2(1) GDPR), including the granting of access to such data. Access to personal data can thus only be granted in accordance with the requirements of the GDPR, namely the principles of transparency and purpose limitation (Article 5 (1)(a) and (b) GDPR), the conditions for the lawfulness of processing, namely consent of the data subjects or legitimate interest of the data controller (Article 6 (1)(a) and (f) GDPR), the information duties (Articles 13(1)(e) and 14 GDPR), and (if applicable) the conditions for the transfer of personal data to third countries (Articles 44 et seqq. GDPR).

If these requirements are met, one can certainly say that granting access to data through compulsory licences is a promising way to establish an adequate free flow of data in the digital single market. Given that many questions still need to be answered, it is also an avenue that deserves further research.

## E CONCLUSION

In order to unlock the potential of the digital economy, the EU promotes its Digital Single Market Strategy. A core aspect of this strategy is establishing an adequate free flow of data within the Union. This adequate free flow balances economic interests of businesses of an entirely free flow of all types of data and individual interests to have some control of the collection and processing of personal data. To achieve this balance, different regulations have been set in place, such as the Trade Secrets Directive, the Open Data, some sector-specific regulations granting access rights, and, above all, the GDPR.

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

These regulatory attempts have been accompanied by a policy discussion on data ownership and data access rights. As shown in this contribution, data ownership can be understood both as a form of property and as a form of control. Both concepts are not equally fit to achieve the goal of establishing an adequate free flow of data within the digital single market. The introduction of data ownership as a property right for personal and non-personal data would increase transaction costs and impede the trading and the use of data. Such a right would thus hinder the EU's goal of achieving a free flow of data. Additionally, in terms of processing personal data, ownership as a property right does not aid individuals to remain in control of their personal data. To the contrary, such ownership rights would substantially weaken their position, as businesses could acquire these rights and exclude the data subjects from using their own personal data. Therefore, the concept of ownership as a property right can be dismissed as a model to help achieve the goals of the Digital Single Market Strategy. The concept of ownership as control has been implemented in the GDPR for the processing of personal data and has the potential to balance economic and individual interests. From an economic perspective, the harmonization of rules and the prohibition of data localization restrictions enhance the free flow of personal data. In contrast, the necessity to comply with the data protection principles (Article 5 GDPR), the need to establish a basis for the lawfulness of all processing of personal data (Article 6 GDPR) and the increased compliance duties of data controllers limit the processing activities and require the establishment of costly organizational and technical solutions to enable data subjects to make use of their individual rights (e.g., right of access and erasure). From an individual perspective, however, these limitations and in particular the (limited) control over how data about them is collected, as well as the options to interfere with the processing of said data at a later stage, are welcomed by many. It remains to be seen, however, whether individuals will actually exercise their (limited) control and whether the current approach of data protection law is able to strike an appropriate balance between economic and individual interests. While some doubts remain, the GDPR can be seen as a first step towards establishing an adequate free flow of personal data within the digital single market.

To achieve the goal of an adequate free flow of data within the EU, individuals and businesses should have access to the data necessary to pursue their interests. For individuals, access to their personal data is key to ensure informational self-determination. Such access is granted by the GDPR, in particular through the right of access and the right to data portability. In most cases, individuals also tend to have sufficient means to access non-personal data that belongs to them. Businesses should have access and be able to use personal and non-personal data as seamlessly as possible in order to develop innovative goods and services and strengthen their competing power, both within the EU and on a global level. The goal of a fully free flow of data, however, must be balanced against the interest of individuals in the protection of their personal data and the interest of businesses in the protection of

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020

their trade secrets. Accordingly, a business' access to personal data held by another business must only be granted in accordance with the GDPR. If these requirements are met or do not apply (as in the case of non-personal data), access to and use of data should be fostered. One way forward is the introduction of additional sector-specific access rights. Another, more all-encompassing and possibly more promising way, is to establish a general right of access to data which is protected as a trade secret by introducing compulsory licences in trade secrets law. Obviously, such licences would only be granted if certain conditions are met, and if an appropriate licence fee is paid. But the mere existence of such licences and the enforcement on a case-by-case basis could help to open up datasets which have been sealed behind corporate walls despite the fact that the data could be useful for others. Overall, the introduction of compulsory licences to grant access to data would allow for the balancing of interests of the businesses holding data with the interests of other businesses that need access to such data to enter a market, develop innovative goods or services, or remain competitive.

Downloaded from https://www.cambridge.org/core. UZH Hauptbibliothek / Zentralbibliothek Zürich (Bill To for 21002 Zurich Uni), on 05 Aug 2021 at 08:07:32, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/9781108919234.020